网络安全技术系列丛书

Maxiumum Security

网络最高安全技术指南

王锐 陈靓 译
靳若明 周刚

机械工业出版社
西蒙与舒斯特国际出版公司

sams net

CMP

网络安全系列丛书

网络最高安全技术指南

王 锐 陈 靓
靳若明 周 刚 译

机 械 工 业 出 版 社
西蒙与舒斯特国际出版公司

本书详细地介绍了计算机网络的安全技术问题，可使您对 Internet 安全知识有一个完整全面的了解。书中对网络安全方面的基础知识，防止“黑客”入侵、各种网络安全工具，防火墙的构成、类型、意义及有关计算机安全性的法律等均有详尽的阐述，并列出了大量的参考资料和网址，供读者查询、参考。

本书可供从事计算机网络安全的管理人员及计算机网络用户使用。

本书版权登记号：图字：01－98－0529

图书在版编目（CIP）数据

网络最高安全技术指南/（美）无名氏著；王锐等译．北京：机械工业出版社，1998.5

（网络安全技术系列丛书）

书名原文：Maximum Security

ISBN 7－111－06224－8

Ⅰ.网… Ⅱ.①无… ②王… Ⅲ.计算机网络－安全技术－指南 Ⅳ.TP393

中国版本图书馆 CIP 数据核字（98）第 05972 号

出 版 人：马九荣（北京市百万庄大街 22 号 邮政编码 100037）

责任编辑：蒋 克

北京第二外国语学院印刷厂印刷·新华书店北京发行所发行

1998 年 5 月第 1 版第 1 次印刷

787mm×1092mm 1/16·35.5 印张

印数：0 001-5 000 册

定价：85.00 元

前　言

我首先介绍一下本书及其用法。严格地说，本书并非一部教材或者使用指南，本书写作的目的是能使你对 Internet 安全知识有一个完整全面的了解。正因如此，它的结构可能不同于以往你所阅读的任何计算机书籍。

尽管本书不能面面俱到，但本书所列的参考资料可以弥补这一切。如果你对 Internet 安全方面的知识知之甚少，你可以按下面的步骤阅读本书，这样做会使你达到最佳的学习效果。

每一章（除了第 1 章）中间都包含有参考资料，其中包括“白皮书”（white paper）、技术报告以及其他一些与讨论内容相关的全面、可靠的信息材料，这些参考资料列举在标有“对照参考”字样的段落里。每当遇到这些资料提示，你应该马上从网上找到这些资料并阅读它，然后再继续书中的内容。在全书的学习过程中，只要始终坚持如一，你将受益匪浅。

我之所以这样组织这本书，是因为 Internet 安全性这个领域不是一成不变的，它的发展变化非常迅速。当然，这个领域中也有一些人人都关心的基本问题，但任何一本书中都不可能包含所有这些内容。不过我们可以在 Internet 上找到以文档形式存放的有关信息资料，这些资料的作者或是 Internet 的开发设计人员，或是其安全性设计人员，他们所从事的工作非常庞大，但他们的文章或技术报告，最多也不超过 40 页（绝大多数都少于 10 页）。

如果只是想略微了解一下 Internet 安全性问题，则不需要阅读这些网上的文件。但假如你想深入了解这方面的知识，那么你可以按照上述步骤进行。

如果你把本书作为一本参考书使用，那么你需要了解一些约定；如果你所需要的资源是一个工具，那么首先下载（download）它（即使它不是为你的平台开发的），然后使用合适的档案管理程序（如 Winzip），你就可以找出该工具携带的文档，这些文档中常包含非常有价值的信息。比如，现在非常著名的扫描器 SATAN（专为 UNIX 设计），其中就有用 HTML 编写的安全指导，它不要求必须有 UNIX 平台（事实上，它仅需要一个浏览器）。许多类似的工具，都包含有文档，文档格式有 PDF、TXT、DOC、PS，以及其他一些可在任何平台上阅读的文件格式。

提示　SATAN 的情况比较特殊，其中有些用 HTML 建立的辅导教程使用 .PL 后缀扩展名，该后缀通常用于标识用 Perl 编写的文档。假如你没有安装 Perl，可以把这种文档转换成原始的 HTML。具体方法是，在文本编辑器上打开文档，把第一行的（<<HTML）替换为<HTML>，然后把文件名后缀改写为 .HTM 或 .HTML，这样，你的浏览器就可以正确地装载页面了。

另外要注意的一点是，本书所列的许多 Internet 文档都以 PostScript 形式存放。PostScript 是一种支持图形和文本的、很不错的解释性语言，主要用于技术领域。要阅读这类文档，需要 PostScript 阅读器（或解释器）。如果你没有 Adobe Illustrator 或是 PostScript 专用软件包，可以使用下列两个应用软件：

■Rops

■Ghostscript/Ghostview

两者都可以很容易地在 Internet 上找到，其中，Rops 位于：

■ftp：//ftp. winsite.com/pub/pc/winnt/txtutil/rops3244.zip

Ghostscript 和 Ghostview 位于：

■ftp：//ftp.cs.wisc.edu/ghost/aladdin/gs353w32.zip

■http：//www.cs.wisc.edu/%7 Eghost/gsview/index.html

这里需要指出的是，Rops 是共享软件，而 Ghostscript 和 Ghostview（以后简称 GS）则不是。这两者的主要不同在于 Rops 更小，更易于安装，运行更快。事实上，它可能是我所见到过的最好的共享软件之一。它在运行时所需要的内存之小令人难以置信，它由英国伦敦的软件工程师 Roger Willcocks 编制。

GS 软件运行相对慢些，但是它支持多种字库以及在不同平台上制作的 Postscript 文档的许多精妙复杂的属性。换言之，有些文档在 Rops 上无法解码，而在 GS 上却可以；GS 对 Postscript 文档的容错能力也较强。如果你没有使用过 PostScript 解释器，可能会遇到一些使你迷惑的情况。比如：解释器无法找到页码，你阅读文档时只能向前翻页（你读到第 2 页便无法返到第 1 页），碰到这种情况，你只能打印文档。

为了避免这种情况，我专门找到备选的文件格式，也就是说，对于每个 PostScript 文档，我都尽量找到对应的 PDF、TXT、DOC、WPG 或者 HTML 文件；但有时我也无法找到其他任何形式的文档（尤其是早期有关 Internet 安全性方面的优秀文章）。如果能找到其他格式的文档，我都会告诉你用它去替换 PostScript 版本，之所以要这样，是因为绝大多数 PC 机用户（Mac 用户除外）一般都没有 PostScript 工具软件。

另外，我要说一下本书中的超级链路（hyperlinks）。书中的每个链路都经过专门的测试。在一些实例中，我提供了对国外文章的链路，这些文章可以在本国找到，我总是尽可能地选择最可靠的链路。所谓可靠的链路，是指那些能够在尽可能短的时间内方便搜寻的链路。也许你不这么认为，但有些国外的链路确实很快。同时，在有些实例中，我只是找到了国外文章的证实性（verified）链路（证实性链路是指我在测试时，所需要的项目确实在 URL 中存在）。为了给你提供最大的帮助，我尽量减少“Object Not Found”字样的出现，当然，费用也不一样。站点（Sites）经常改变它们的结构，所以有些链路不再有效（尽管绝大多数链路在本书印刷前一两个月才测试过）。

同时，许多超链路路径在书中都用全称表示，对每个目标，都给出它的全称表示，而不是仅列出它所属的服务器。关于可加载的文件（通常是工具），这些链路提供给你的不是一个页面，而是在你的机器上启动下载过程，把文件直接提供给你。这样做可以节省你的时间，但可能会迷惑一些新手；当出现一个对话框，问你是否保存文件时，不必大惊小怪。

请注意本书中我指出的每一个工具或软件的编程语言。所述的许多工具在创建和使用前都需要一个编译器或解释器。如果你现在没有这种编程语言或者必要的解释器（或者你的平台不同于某一工具的目标平台），那么请重新查阅参考手册。除非这些工具中包含着对你有价值的文档，否则你可能要停止下载它。另外，许多应用程序都只有源码形式，尽管大多数源码我都亲自检查过，但我不能保证它们都正确无误。如果你想在自己的机器上加载源码并编译它，要清楚我和 Sams 出版社对这些文件中可能存在的陷阱和有害代码不负任何责任。

大多数参考文件都来源可靠，其中许多都有数字化签名、PGP 密钥或其他保密手段，以确保文件的可靠性和完整性。但是，那些源于“闯入者”站点（site）的代码可能不“干净”，这时要靠你自己判断。

> **注意** Windows 和 Mac 用户特别注意：如果你还弄不清我正谈什么，不用害怕，到了第 6 章“TCP/IP 简短入门”会好起来的。我尽一切可能使这本书对所有读者来说都简单易懂，尽一切努力解释全书众多的术语和过程。如果你了解这些定义，可跳过不看；如果你不了解，请仔细阅读。

所列的大多数站点都可方便地访问；还有一些站点需要使用桌面结构或全图形接口，那些没有这些接口的浏览器可能无法访问这些站点。不过，这种站点很少；我也会尽可能去找到备选页面（即支持非桌面浏览器的页面），这样几乎所有页面都可用任何浏览器访问。但事情不可能十全十美，也会出现例外，对此，我深表歉意。

对于我认为“非常好”的站点，切记：这只是我的个人意见。如果一个站点能提供很专业的信息或者给出许多有价值的建议，我便认为它“好”。当然，这并不意味着我未提过的站点就“不好”，这里的每一个站点都是我精心挑选的，都能提供有关安全性的有用信息。那些我认为“特别好”的站点，它们在提供信息方面确实堪称典范。

关于超级链路，要说明的一点是：在附录 A 的末尾，“在哪里得到更多的信息”，我列出了一系列超级链路清单，只有名单，没有评述，相当于一个庞大的书签文件。这样做的目的，在附录中我已详细阐明，这里我想简单说几句，这个清单（CD－ROM 中也能看到）是提供给安全性方面的专业学生的；通过把这个清单装入个人自动机（Clearweb 就是很好的一例），你可以在自己的本地机上建立一个庞大的安全库，这种自动机可以搜索目录中的页面，寻找你所定义的任何文件类型。对于那些有足够磁盘空间，正想建立一个安全库的公司来说，这一切都可自动完成。大多数自动机可在几分钟内“克隆（clone）（即仿制）出一个远程站点。

要知道，这里的绝大多数链路自己会产生许多链路的页。因此，如果你要运行自动机，最好要有足够的磁盘空间供输出。如果你想按原格式打印它们，那么打印清单中所有可搜寻到的文档（如果用自动机搜寻每一个链路的话）将用掉近 7ft. 高的纸，我这样做过，所以我很清楚。在附录 A 中，我描述了这个过程。如果你想从所列的全部站点中搜寻并打印书面信息及二进制代码，你要在两星期内得到 Internet 上绝大部分的书面形式的安全性知识。在从事重要的安全性研究的组织中，这样做非常有意义，尤其是把所有文件都重新组织为单文本格式（你可以做一个特别的索引，等等）。

这里所提到的有些书籍或文档无法“在线”（online）获得，但这些文档可以设法找到。总之，我尽可能地提供有关信息。有时包含 ISBN 或 ISSN，有时不包含；ISBN 不一定总能得到，在这种情况下（尽管很少），我会提供国立图书馆的分类号或其他能够帮助你找到参考资料的信息。任何无法寻到的资料（从网上或其他地方）本书都忽略不提。

此外，我尽一切可能地相信作者本人或者有技术价值的通信信息，这其中包括 Usenet 新闻机构的邮件、邮件列表、Web 页面和其他媒介。几乎所有情况下（除了附录 B“安全咨询顾问”中出现的销售商名单外），我都省略了机构的 e－mail 地址。你也许会在不同的站点获得这些地址，但我决不在本书中印出它们，我尽一切努力尊重这些个人隐私。

附录 B 中的销售商名单不是从本地的电话簿上得到的。1997 年 3 月，我向几家重要的安全机构发了电子邮件，索取到了本书中所列的销售商地址。这些销售商（和销售公司）都是合格的安全性方面的销售商和顾问。这些人每天都可以提供安全方面的产品和服务。其中很多人经营经过国防级系统评估的产品和一些典型的安全环境产品，他们只是这类公司的一小部分代表。本名单中未列的销售商，并不意味着他们不合格。这仅仅说明他们不愿意被列在一个匿名者所写的书中，安全领域的人们小心谨慎是自然的事，无可非议。

最后，我有几点建议。附录 C“一个隐藏信息”中指出了 CD－ROM 中一块加密的文字，它们是用 PGP 加密的。如果你将它解密，你将发现一个声明，这个声明揭示了 Internet 中一个尚未广为人知的组成部分。但 5 年内，这个组成部分对大多数个人来说将变得很透明。这里你需要知道关于这个加密声明的几个事情。

首先，加密的文字只包含我的意见，不是 Sams.net 出版社的意见。事实上，为了确保 Sams.net 出版社与该声明无关，我预先告知拒绝向 Sams.net 工作人员提供这个密码，所以他们绝对不了解声明的内容。同样，我向你保证（就像我向 Sams.net 保证那样），声明中不含有任何褒渎性的语言或是其他任何被认为是不宜于某一年龄段读者的东西。声明相当直截了当地、客观地提醒每一个人，包括安全专家都极为忽略的 Internet 的一个方面。这个方面极其重要，不单单对美国人，对世界各国的人们也是如此。从根本上讲，这个声明是一个预言。

现在说说如何解密该声明。该声明本身非常不易破解，因为我用了最高级的加密手段。但是，你可以用间谍行业中曾经很常用的技术找到密码。在附录 C 中，有几行清晰的文字是由一串用分号分开的字符组成的（分号是分隔符），一旦你识别出这些字符的意义，你会发现一些有趣的可能性，在你一一尝试之后，你将最终解开这个声明（这几行清晰的文字揭示了密码）。你如果聪明，会很容易地解开这个谜（当然，这对 NSA 那些疯狂的人没有问题，只要他们是成年人而不是孩子，这是我提供的唯一线索）。该信息的公开钥匙是 root@netherworld.net。

如果你破解了这个信息，应该把它呈献给国会议员，对于这群绝大部分不懂 Internet 的人来说，这段加密文字中的信息是极其重要的。

祝好运！

作者简介

作者把他自己描述成一个“UNIX 螺旋桨头部”，一个 Perl 编程语言、Linux 和 FreeBSD 的忠实拥护者。

作者在加利福尼亚两家健康服务公司当了 4 年的系统管理人员。之后，便开始了他自己的安全咨询生意。现在，他专门测试各种网络平台的安全性，即闯入计算机网络，并发现导致非法闯入的“漏洞”（hole），这其中包括 Novell NetWare、Microsoft Windows NT、Sun OS、Solaris、Linux 和 Microsoft Windows 95，但不局限于此。目前，他的主要任务是负责一个横跨洛杉矶到蒙特利尔的广域网的安全。

现在，作者同他的妻子平静地生活在南加利福尼亚州，他的家中有一台 Sun SPARC 工作站，一台 IBM RS/6000，两台 Pentiums，一台 Macintosh 和一台 MicroVAX 机。

在 80 年代末，作者曾因开发了一种破坏银行自动取款机系统安全性的技术，而被控犯有一系列经济罪行，因此作者选择使用匿名写书。

告诉我们您的想法

读者是我们图书最重要的评判人。通过您的意见，我们可以了解需要坚持或改进的地方，可以了解您的需要以及您的高见。您可以帮助我们出版您所需要的好书和计算机指南。

您访问过 CompuServe 或是 WWW 吗？在任何提示下，敲入 GO SAMS 就可以查出我们的 CompuServe 论坛（forum），如果您更喜欢 WWW，您可以在 http：//www.mcp.com 上查出我们的站点。

注意

关于本书，如果您有什么技术问题，请拨打技术热线 317－581－4669。

作为本书创作组的负责人，我欢迎你的批评指教。您可以通过电传、电子邮件或信件直接与我联系，发表您对本书的看法，帮助我们改进工作。通讯地址如下：

电　　传　317－581－4669

电子邮件　Mark Taber

programming _ mgr@sams.mcp.com

通迅地址　Mark Taber

Comments Department

Sams Publishing

201W.103rd Street

Indianapolis，IN 46290

目　录

第三部分 工 具

第四部分 平台和安全性

第五部分 从基本开始

第六部分 远 程 攻 击

第七部分 法 律

第八部分 附 录

第一部分 基 础 篇

第 1 章 本书的写作目的

计算机网络中的“入侵”活动已经引起了公众的高度重视。有关国际互联网（Internet）的入侵者和破坏者的报道经常见诸于报端，图书出版商们也随之竞相出版发行有关这方面主题的书籍。值得称道的是，出版界没有动摇过这种决心，书店书架上有关网络安全方面的书籍数量猛增。然而公众依然很谨慎，他们认识到这其中的商业动机，因而，他们对像本书这样一类的书籍持怀疑态度也是可以理解的。其实他们只需要浏览一下本地书店的书架，就可以准确地估计形势。

关于 Internet 安全方面的书籍存在共同之处，防火墙（firewall）技术似乎在其中占主导地位。在这类书籍中，内容往往很分散，并且局限于一个很窄的产品范围内。作者一般通篇照搬那些可以在网上轻松获得的陈旧和过时的文章，这使得这些文章都不切合实际，因为有实践经验的读者都已掌握了这些参考资料的内容，而没有经验的读者又用不上它，因此，人们觉得这些书没有多大用处。在美国的街边书店里，有关 Internet 安全方面的书籍销售情况不好。

造成这类书籍滞销的另一个原因是，大家错误地认为要进行网络“入侵”，首先一定是一个天才或者 UNIX 权威，其实这种观点是错误的。诚然，有些开发活动需要具备目标操作系统的高级知识，但是许多现有操作系统环境中的应用程序，可以使这些开发活动变得很简单。尽管如此，人们依然对网络“入侵”感到很神秘，对花费 40 美元买本有关“入侵”的书持谨慎态度。

所以，在出版本书之初，Sams.net 出版社经历了一个相当不寻常的过程。Sams.net 出版社在信息领域具有一定的权威性。据我所知，超过 2/3 的专业人员都购买过该出版社出版的书籍。正因为如此，对他们而言，本书具有一定的特殊性。

“破解”、“入侵”以及网络安全性都是“爆炸性”（explosive）题目。出版一本 C++ 入门和出版一本网络“入侵”指南是极其不同的，像本书这样的读物包含着一定的危险性：

- 读者可能恶意地使用书中内容。
- 可能引起最秘密的 Internet 安全机构的不满。
- 可能引起那些尚未修补好自己软件中漏洞的软件销售商的不满。

如果其中的任何危险成为现实，那么 Sams.net 出版社将受到调查，甚至是非难。既然如此，为什么 Sams.net 出版社又要出版发行此书呢？

Sams.net 出版社出版此书（我也同意写此书），是因为这是实际需要。我愿意费些功夫来解释这种需要，因为它在 Internet 世界中引起了一些争论。许多人认为这种需要是商业性质的需要，是专营安全产品的软件销售商虚构出来的，这种指责——读者不久将会发现——是不能成立的。